CLAIMS

1. A data processing apparatus for initially generating a verifying value for verifying an individual contents data to be stored in a memory device, then storing said verified value in said memory device in correspondence with said contents data, and finally checking to probe actual occurrence or absence of the act of tampering with said contents data by referring to said verifying value; wherein

said verifying value is independently generated and stored in said memory device per category of contents data.

2. The data processing apparatus according to Claim 1, wherein

said data processing apparatus computes a verifying value based on data of the objective contents data, then compares the computed verifying value to a previously stored verifying value, and finally utilizes the corresponding contents data solely in the case in which both values are identified to be coincident with each other in case of utilizing the contents data.

3. The data processing apparatus according to Claim 1, wherein

said memory device stores such contents data of a variety of categories corresponding to a plurality of directories; and

said verifying value is generated to deal with an assemblage of contents data individually corresponding to said plural directories.

4. The data processing apparatus according to Claim 1, wherein

said memory device comprises a flash memory; and

said verifying values per category are stored in such a domain preset as a utilization inhibited block in said flash memory.

5. The data processing apparatus according to Claim 1, wherein

said categories are individually provided per kind of contents data, and

each category presets and stores independent verifying values per kind of contents data.

6. The data processing apparatus according to Claim 1, wherein

said categories are individually preset based on a controlling entity of an enabling key block which enciphers a contents key functioning as a contents enciphering key and then delivers said contents key to a specific device; and

said categories individually preset and store such verifying values being independent from each other per controlling entity of said enabling key block.

7. The data processing apparatus according to Claim 1, wherein

said verifying values are individually generated based on message authentication codes which are generated by applying the Data Encryption Standard to partial data message constituting a contents related data such as contents data and header data respectively to be subject to verification via said verifying values.

8. A data processing apparatus which generates and stores message authentication codes functioning themselves as the data for probing the act of tampering with contents data or header data stored in a memory device; wherein

said data processing apparatus generates a plurality of message authentication codes in such mutually different data domains in contents data or header data;

part of said data domains for generating said message authentication codes therein is utilized as a common data; and

whenever renewing any of said plural message authentication codes, said common data is also renewed to further renew other message authentication codes as well.

9. A data processing method for initially generating a verifying value for verifying an individual contents data to be stored in a memory device, then storing said verified value in said memory device in correspondence with said contents data, and finally checking to probe actual occurrence or absence of the act of tampering with said contents data by referring to said verifying value; wherein

said verifying value is independently generated and stored in said memory device per category of contents data.

10. The data processing method according to Claim 9, wherein

said data processing method computes a verifying value based on data of the objective contents data, then compares the computed verifying value to a previously stored verifying value, and finally utilizes the corresponding contents data solely in the case in which both values are identified to be coincident with each other in case of utilizing the contents data.

11. The data processing method according to Claim 9, wherein

said memory device stores such contents data of a variety of categories corresponding to a plurality of directories; and

said verifying value is generated to deal with an assemblage of contents data individually corresponding to said plural directories.

12. The data processing method according to Claim 9, wherein

said memory device comprises a flash memory; and

said verifying values per category are stored in such a domain preset as a utilization inhibited block in said flash memory.

13. The data processing method according to Claim 9, wherein

said categories are individually provided per kind of contents data, and

each category presets and stores independent verifying values per kind of contents data.

14. The data processing method according to Claim 9, wherein

said categories are individually preset based on a controlling entity of an enabling key block which enciphers a contents key functioning as a contents enciphering key and then delivers said contents key to a specific device; and

said categories individually preset and store such verifying values being independent from each other per controlling entity of said enabling key block.

15. The data processing method according to Claim 9, wherein

said verifying values are individually generated based on message authentication codes which are generated by applying the Data Encryption Standard to partial data message constituting a contents related data such as contents data and header data respectively to be subject to verification via said verifying values.

16. The data processing method according to Claim 15, wherein

said contents data and header data subject to verification individually contain a plurality of message authentication codes generated in different data domains;

part of said data domains for generating said message authentication codes therein is utilized as a common data; and

whenever renewing any of said plural message authentication codes, said common data is also renewed to further renew other message authentication codes as well.

17. A data processing method which generates and stores message authentication codes functioning themselves as the data for probing the act of tampering with contents data or header data stored in a memory device; wherein

said data processing apparatus generates a plurality of message authentication codes in such mutually different data domains in contents data or header data;

part of said data domains for generating said message authentication codes therein is utilized as a common data; and

whenever renewing any of said plural message authentication codes, said common data is also renewed to further renew other message authentication codes as well.

18. A recording medium recorded with a computer program operable to store verifying values for verifying contents data in a memory device in correspondence with individual contents data and to provide a computer system with the computer program for probing actual occurrence or absence of the act of tampering with contents data on a computer system; wherein

said computer program comprises a step of generating and storing such verifying values being independent per category of contents data.